Council of the European Union

Brussels, 10 July 2026
(OR. en)

11772/26
ADD 1

SOC 490
ANTIDISCRIM 73
FREMP 243
TRANS 497
SPORT 38
CULT 94
DELACT 110

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	1 July 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	C(2026) 4534 annex
Subject:	ANNEXES to the COMMISSION DELEGATED REGULATION (EU) .../... supplementing Directive (EU) 2024/2841 as regards setting the QR code on the physical version of the European Disability Card and setting the QR code and establishing common technical specifications that ensure the security of the physical version of the European Parking Card for persons with disabilities, as well as interoperability matters

EUROPEAN
COMMISSION

Brussels, 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

ANNEXES

to the

COMMISSION DELEGATED REGULATION (EU) .../...

supplementing Directive (EU) 2024/2841 as regards setting the QR code on the physical version of the European Disability Card and setting the QR code and establishing common technical specifications that ensure the security of the physical version of the European Parking Card for persons with disabilities, as well as interoperability matters

ANNEX I

QR CODE SPECIFICATIONS FOR THE PHYSICAL VERSION OF THE EUROPEAN DISABILITY CARD

1. **Format of the QR code for the physical version of the European Disability Card (EDC)**

(a) **QR code Model 2 format**, in accordance with the international QR code specifications ISO/IEC 18004:2024 or equivalent.

(b) **Error Correction Level M** (15% redundancy) ensuring resilience to scratches or partial damage of a printed QR code.

(c) **Encoding Mode:** The QR payload shall consist of the combined issuerSigned Concise Binary Object Representation (CBOR) structure and the corresponding issuerAuth COSE_Sign1 signature object as defined in CBOR Object Signing and Encryption (COSE, RFC 9052 Sections 3.1, 4.2 and 4.4), following the mDOC data-model pattern for issuerSigned items, but adapted for static physical-card use. The issuerAuth shall be a COSE_Sign1 object with alg = ES256 and a protected header containing x5t (the COSE X.509 certificate hash header parameter defined in RFC 9360 (section 2); for interoperability, the hash algorithm used in x5t shall be SHA-256).

(d) Prior to QR code encoding, the combined CBOR/COSE object shall be **compressed using zlib format** (RFC 1950, section 2.2) **with the deflate** algorithm (RFC 1951 sections 3.2 and 4). The resulting compressed byte array shall be encoded in **QR code Byte Mode**, ensuring full support for binary CBOR/COSE payloads and scanner interoperability.

For all text fields included in the QR payload, issuers shall encode characters as Unicode UTF-8 within CBOR text strings. Transliteration shall not be applied to signed payload data. For interoperability purposes, issuers shall apply Unicode Normalisation Form C (NFC) to all textual fields before signing.

(e) **Prefix:** The EDC QR string shall begin with “ED1:MDOC:”. This identifies card type and encoding profile. Prefixes are case-sensitive and must be present. Unknown or unsupported prefixes shall cause rejection. The prefix and the compressed payload shall be encoded as a single Byte Mode data segment in the QR code.

(f) **Minimum Module Size ≥ 0.25mm** to ensure readability on printed cards.

(g) **Maximum Version 20;** with up to 97 × 97 modules on each side.

2. **EDC Signature Generation Specifications**

The qualified electronic seal (QSeal) used to seal EDC QR codes ensures that the encoded data originate from the authorised issuing authority and have not been altered.

(a) **Signature Algorithm**: The signature algorithm shall be ES256 (Elliptic Curve Digital Signature Algorithm (ECDSA) with SHA-256 using the P-256 curve), as defined in RFC 9053 (section 2.1); in COSE, the algorithm is identified by the alg header parameter in RFC 9052 (section 3.1).

(b) **Signing Key**: The QR payload shall be signed using the private key corresponding to a Qualified Certificate for Electronic Seal (QSealC).

(c) **COSE Structure:** The signature container shall be a COSE_Sign1 object. The protected header shall include alg (ES256) and x5t (the COSE X.509 certificate hash header parameter defined in RFC 9360 (section 2); for interoperability, the hash algorithm used in x5t shall be SHA-256). Verification shall rely on using the x5t value to locate the corresponding certificate in the verifier's locally cached trust store built from Trusted List information and shall then validate the certificate chain and certificate status in accordance with the eIDAS trust framework.

(d) **Signature Standard**: The QR code payload shall be signed as a COSE_Sign1 object in accordance with RFC 9052 (section 4), CBOR Object Signing and Encryption. The COSE_Sign1 object shall be carried in issuerAuth and encoded without the CBOR tag for COSE_Sign1. The payload field of the COSE_Sign1 object shall be detached and encoded as CBOR null. For signature generation and verification, the external payload shall be the deterministic-CBOR encoded structure containing the docType value and the issuerSigned value from the top-level CBOR map.

(e) **Hash Algorithm**: SHA-256 shall be used as part of ES256 for signature generation and integrity verification.

(f) **Encoding**: The payload shall be encoded using CBOR (RFC 8949, section 4.2), as required by the COSE and mDOC specifications, ensuring encoding and reproducibility of the signed data.

3. **Printing Specifications**

(a) **Quiet Zone**: A clear margin of **4 modules** shall surround the QR code on all sides, free of any print, pattern, or background.

(b) **Contrast**: QR code shall be printed on a white background, with a minimum contrast ratio of **4:1**, to ensure high readability under varying lighting conditions.

(c) The QR code shall be printed using the colour defined in Annex I to Directive (EU) 2024/2841 that ensures maximum contrast.

(d) **Placement and Size**: The QR code, including the quiet zone, shall be 26.25 mm × 26.25 mm, located on the reverse side of the card at the bottom-right corner. The QR code shall be maximum Version 20 (97 × 97 modules), with a module size of 0.25 mm or larger.

The QR code, including its quiet zone, shall be positioned at least 5 mm from the right-hand edge and at least 5 mm from the bottom edge of the card.

4. **Data in the EDC QR code**

The QR code shall contain a minimal, offline-verifiable dataset in compliance with the data minimisation principle laid down in Article 5(1), point (c), of Regulation (EU) 2016/679. The payload structure shall be as follows:

(a) Card attributes are encoded in CBOR within an issuerSigned object.

(b) The structure is wrapped and signed by the issuing authority's QSeal as an issuerAuth (COSE_Sign1, ES256, including x5t, the COSE X.509 certificate hash header parameter).

(c) The resulting CBOR / COSE object shall be compressed in accordance with point 1(d) of this Annex. The QR code payload shall consist of the prefix "ED1:MDOC:", followed by the

resulting compressed byte array, and the complete payload shall be encoded using Byte Mode as a single QR code data segment.

Data contents shall consist of a sub-set of visible data from the front card fields listed in Annex I to Directive (EU) 2024/2841 (name, surname, card serial number, expiry date), together with the revocation identifier, electronic signature, and schema information.

Electronic signature shall contain:

(i) issuerAuth - A COSE_Sign1 object signed with the issuing authority's **QSealC private key**.

(ii) protected header that includes alg = ES256 (signature algorithm) and x5t (the COSE X.509 certificate hash header parameter).

5. Optional Data

No optional data shall be included in the QR code.

6. Revocation Identifier (RID)

In addition to the visible card serial number the QR code shall include a dedicated revocation identifier (RID).

The RID shall be used for determining revocation status and for revocation list management. The RID shall not be printed on the card and it shall not be displayed to the card verifiers.

6.1. *Requirements for the RID*

The RID shall:

(a) be included in the signed QR payload;

(b) be unique at least within the issuing authority's issuance domain;

(c) not be printed on the card and not intended to be human readable;

(d) not reveal personal data and not be directly meaningful;

(e) not be directly derivable from the visible card serial number; and

(f) be cryptographically bound to the QR payload by the qualified electronic seal.

6.2. *RID format and size*

The RID shall be encoded as a CBOR byte string (bstr). The RID shall be 16 bytes (128 bits) in length.

The RID shall be generated by the issuing authority using a method under its control that ensures sufficient entropy and resistance to guessing or enumeration.

6.3. *Revocation Lists*

Revocation lists published for verification purposes shall reference only the RID of revoked cards. Card serial numbers shall not be published in revocation lists.

7. CBOR payload (inside the QR code) of EDC

Only the following data shall be included inside the QR payload, consistent with the visible EDC data fields laid down in Annex I to Directive (EU) 2024/2841.

Top level contents:

(a) docType = "eu.edc"

(b) issuerSigned.nameSpaces."eu.edc" with attributes shown in table below

(c) issuerAuth = COSE_Sign1 (QSeal)

Field	**mDOC path**	**Type/Format**
Data schema version	issuerSigned.nameSpaces."eu.edc".ver	String (e.g., "1.0")
Card type: EDC	docType	Enum ("eu.edc")
Card Serial Number	issuerSigned.nameSpaces."eu.edc".sub	String
Revocation Identifier	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bytes)
First name of cardholder	issuerSigned.nameSpaces."eu.edc".givenName	Unicode text string (UTF-8)
Surname of cardholder	issuerSigned.nameSpaces."eu.edc".familyName	Unicode text string (UTF-8)
Expiry date of card	issuerSigned.nameSpaces."eu.edc".exp	CBOR tag 1004, as defined in RFC 8943 (section 2.1), containing a UTF-8 text string representing an RFC 3339 full-date in YYYY-MM-DD format.

The electronic signature is carried in issuerAuth (a COSE_Sign1 object). The certificate chain shall not be embedded in the QR code payload; instead, the protected COSE header shall include x5t, a certificate thumbprint used to locate the corresponding QSealC in the verifier's cached trust store.

8. EDC QR code payload example: commented JavaScript Object Notation-style logical representation

The following example is a human readable JavaScript Object Notation (JSON) representation of the EDC logical view. In practice, this structure shall not be human readable as it shall be:

(a) Encoded in CBOR (RFC 8949, section 3);

(b) Signed using untagged COSE_Sign1 structure with a detached payload (RFC 9052, section 4.),

(c) include the expiry date as a CBOR tag 1004 full-date value in accordance with RFC 8943 (section 2.1);

(d) include the x5t protected-header parameter in accordance with RFC 9360, using SHA-256 over the DER-encoded end-entity QSealC; and

(e) compressed and prefixed with the string ED1:MDOC: before being encoded in the QR code.

```
{
 // JSON-style, human-readable EDC logical view only.
 // Actual QR payload is deterministic CBOR, not JSON.
 "docType": "eu.edc", // EDC credential. The docType value is included, together with
  //issuerSigned, in the COSE_Sign1 external payload.

 "issuerSigned": {
  // Data protected by issuerAuth; used as detached payload.
  // For signature generation and verification, the detached external payload covers both
  // docType and issuerSigned.
  "nameSpaces": {
   "eu.edc": {
    "ver": "1.0", // QR profile/schema version

    // Card serial number; issuer-defined, max. 24 characters.
    "sub": "AB1234567890123456789OCD",
```

```
      // Revocation identifier: actual CBOR bstr, 16 bytes/128 bits.
      // Shown here as 32 hex characters for readability.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Ann",    // first name printed on the EDC
      "familyName": "Other", // surname printed on the EDC

      // Actual CBOR encoding uses tag 1004 for RFC 3339 full-date.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Actual form: untagged COSE_Sign1, not a JSON object.
  "type": "COSE_Sign1",
  "tagged": false,       // encoded without COSE_Sign1 CBOR tag
  "payload": "detached", // COSE payload field is CBOR null

  "protectedHeader": {
    // alg: ES256; equivalent COSE header parameter 1 = -7.
    "alg": "ES256",

    // x5t: certificate thumbprint; COSE header parameter 34.
    "x5t": {
      "hashAlg": "SHA-256", // equivalent COSE hash value -16
```

```
      // SHA-256 hash of DER-encoded end-entity QSealC.
      // 32 bytes represented as 64 hex characters.
      "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // empty in this example

  // ES256 COSE signature: 64 bytes = 128 hex characters.
  "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

9. Use of cryptographic mechanisms

The use of cryptographic mechanisms in the context of this Annex shall be in compliance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by the European Union Agency for Cybersecurity (ENISA).

ANNEX II

QR CODE SPECIFICATIONS FOR THE PHYSICAL VERSION OF THE EUROPEAN PARKING CARD FOR PERSONS WITH DISABILITIES

1. **Format of the QR code on the physical version of the European Parking Card for persons with disabilities (EPC)**

(a) **QR code Model 2 format**, in accordance with the international QR code specifications ISO/IEC 18004:2024 or equivalent.

(b) **Error Correction Level M** (15% redundancy) ensuring resilience to scratches or partial damage of printed QR code.

(c) **Encoding Mode:** The QR payload shall consist of the combined issuerSigned Concise Binary Object Representation (CBOR) structure and the corresponding issuerAuth COSE_Sign1 signature object as defined in CBOR Object Signing and Encryption (COSE, RFC 9052 Sections 3.1, 4.2 and 4.4), following the mDOC data-model pattern for issuerSigned items, but adapted for static physical-card use. The issuerAuth shall be a COSE_Sign1 object with alg = ES256 and a protected header containing x5t (the COSE X.509 certificate hash header parameter defined in RFC 9360 (section 2); for interoperability, the hash algorithm used in x5t shall be SHA-256).

(d) Prior to QR code encoding, the combined CBOR/COSE object shall be **compressed using zlib format (RFC 1950, section 2.2) with the deflate** algorithm (RFC 1951, sections 3.2 and 4). The resulting compressed byte array shall be encoded in **QR code Byte Mode**, ensuring full support for binary CBOR/COSE payloads and scanner interoperability.

For all text fields included in the QR payload, issuers shall encode characters as Unicode UTF-8 within CBOR text strings. Transliteration shall not be applied to signed payload data. For interoperability purposes, issuers shall apply Unicode Normalisation Form C (NFC) to all textual fields before signing.

(e) **Prefix**: The EPC QR string shall begin with “EP1:MDOC:”. This identifies card type and encoding profile. Prefixes are case-sensitive and must be present. Unknown or unsupported prefixes shall cause rejection. The prefix and the compressed payload shall be encoded as a single Byte Mode data segment in the QR code.

(f) **Minimum Module Size ≥ 0.35mm** to ensure readability on printed cards.

(g) **Maximum Version 20**; with up to 97 x 97 modules on each side.

2. **EPC Signature Generation Specifications**

The qualified electronic seal (QSeal) used to seal EPC QR codes ensures that the encoded data originate from the authorised issuing authority and have not been altered.

(a) **Signature Algorithm**: The signature algorithm shall be ES256 (ECDSA with SHA-256 using the P-256 curve), as defined in RFC 9053 (section 2.1); in COSE, the algorithm is identified by the alg header parameter in RFC 9052 (section 3.1).

(b) **Signing Key**: The QR payload shall be signed using the private key corresponding to a Qualified Certificate for Electronic Seal (QSealC).

(c) **COSE Structure**: The signature container shall be a COSE_Sign1 object. The protected header shall include alg (ES256) and x5t (the COSE X.509 certificate hash header parameter defined in RFC 9360 (section 2) ; for interoperability, the hash algorithm used in x5t shall be SHA-256). Verification shall rely on using the x5t value to locate the corresponding certificate in the verifier's locally cached trust store built from Trusted List information and shall then validate the certificate chain and certificate status in accordance with the eIDAS trust framework.

(d) **Signature Standard**: The QR code payload shall be signed as a COSE_Sign1 object in accordance with RFC 9052 (section 4), CBOR Object Signing and Encryption. The COSE_Sign1 object shall be carried in issuerAuth and encoded without the CBOR tag for COSE_Sign1. The payload field of the COSE_Sign1 object shall be detached and encoded as CBOR null. For signature generation and verification, the external payload shall be deterministic-CBOR encoded CBOR structure containing the docType value and the issuerSigned value from the top-level CBOR map.

(e) **Hash Algorithm**: SHA-256 is used as part of ES256 for signature generation and integrity verification.

(f) **Encoding**: The payload shall be encoded using CBOR (RFC 8949, section 4.2), as required by the COSE and mDOC specifications, ensuring encoding and reproducibility of the signed data.

3. **Printing Specifications**

(a) **Quiet Zone**: A clear margin of **4 modules** shall surround the QR code on all sides, free of any print, pattern, or background.

(b) **Contrast**: QR code shall be printed on a white background, with a minimum contrast ratio of **4:1**, to ensure high readability under varying lighting conditions.

(c) The QR code shall be printed using the colour defined in Annex II to Directive (EU) 2024/2841 that ensures maximum contrast.

(d) **Placement and Size:** The QR code, including the quiet zone, shall be **37 mm × 37 mm**, located on the front of the card, slightly off-centre to the right, towards the bottom edge. The QR code shall be maximum version 20 (97 × 97 modules), with module size of 0.35 mm or larger.

The QR code, including its quiet zone, shall be positioned at least 5 mm from the bottom edge of the card.

4. **Data in EPC QR code**

The QR code shall contain a minimal, offline-verifiable dataset in compliance with the data minimisation principle contained in Article 5(1), point (c), of Regulation (EU) 2016/679. The payload structure is as follows:

(a) Card attributes are encoded in CBOR within an issuerSigned object.

(b) This structure is wrapped and signed by the issuing authority's QSeal as an issuerAuth (COSE_Sign1, ES256, including x5t, the COSE X.509 certificate hash header parameter).

(c) The resulting CBOR / COSE object shall be compressed in accordance with point 1(d) of this Annex. The QR code payload shall consist of the prefix "EP1:MDOC:", followed by the

resulting compressed byte array, and the complete payload shall be encoded using Byte Mode as a single QR code data segment.

Data contents shall consist of a sub-set of visible data from the front card fields listed in Annex II of Directive (EU) 2024/2841 (expiry date, card serial number), together with the revocation identifier, electronic signature, and schema information.

Electronic signature shall contain:

(i) issuerAuth - A COSE_Sign1 object signed with the issuing authority's **QSealC private key**.

(ii) Protected header that includes alg = ES256 (signature algorithm) and x5t (the COSE X.509 certificate hash header parameter).

5. Optional Data

No optional data shall be included in the QR code.

6. Revocation Identifier (RID)

The Revocation Identifier of the EPC shall comply with point 6 of Annex I.

Revocation lists for revoked EPCs shall reference only the RID. Card serial numbers shall not be published in revocation lists.

7. CBOR payload (inside the QR) of EPC

Only the following data shall be included inside the QR payload, which is consistent with the visible EPC card fields set out in Annex II to Directive (EU) 2024/2841:

Field	**mDOC path**	**Type/Format**
Data schema version	issuerSigned.nameSpaces."eu.epc".ver	String (e.g., "1.0")
Card type: EPC	docType	Enum ("eu.epc")
Card Serial Number	issuerSigned.nameSpaces."eu.epc".sub	String
Revocation Identifier	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bytes)
Expiry date of card	issuerSigned.nameSpaces."eu.epc".exp	CBOR tag 1004, as defined in RFC 8943 (section 2.1), containing a UTF-8 text string

		representing an RFC 3339 full-date in YYYY-MM-DD format.

The electronic signature shall be carried in issuerAuth (a COSE_Sign1 object). The certificate chain shall not be embedded in the QR code payload; instead, the protected COSE header shall include x5t, a certificate thumbprint used to locate the corresponding QSealC in the verifier's cached trust store.

8. EPC QR code payload example: commented JavaScript Object Notation-style logical representation

The following example is a human readable JavaScript Object Notation (JSON) representation of the EPC logical view. In practice, this structure shall not be human readable as it shall be:

(a) Encoded in CBOR (RFC 8949, section 3),

(b) Signed using untagged COSE_Sign1 structure , with a detached payload (RFC 9052, section 4),

(c) include the expiry date as a CBOR tag 1004 full-date value in accordance with RFC 8943 (section 2.1);

(d) include the x5t protected-header parameter in accordance with RFC 9360, using SHA-256 over the DER-encoded end-entity QSealC; and

(e) compressed and prefixed with the string EP1:MDOC: before being encoded in the QR code.

```
{
 // JSON-style, human-readable EPC logical view only.
 // Actual QR payload is deterministic CBOR, not JSON.
 "docType": "eu.epc", // EPC credential. The docType value is included, together with
  //issuerSigned, in the COSE_Sign1 external payload.

 "issuerSigned": {
  // Data protected by issuerAuth; used as detached payload.
  // For signature generation and verification, the detached external payload covers both
```

```
  // docType and issuerSigned.
  "nameSpaces": {
    "eu.epc": {
      "ver": "1.0", // QR profile/schema version

      // Card serial number; issuer-defined, max. 24 characters.
      "sub": "EF12345678901234567890GH",

      // Revocation identifier: actual CBOR bstr, 16 bytes/128 bits.
      // Shown here as 32 hex characters for readability.
      "rid": "4a8d9c112233445566778899aabbccdd",

      // Actual CBOR encoding uses tag 1004 for RFC 3339 full-date.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Actual form: untagged COSE_Sign1, not a JSON object.
  "type": "COSE_Sign1",
  "tagged": false,       // encoded without COSE_Sign1 CBOR tag
  "payload": "detached", // COSE payload field is CBOR null

  "protectedHeader": {
    // alg: ES256; equivalent COSE header parameter 1 = -7.
    "alg": "ES256",
```

```
    // x5t: certificate thumbprint; COSE header parameter 34.
    "x5t": {
      "hashAlg": "SHA-256", // equivalent COSE hash value -16

      // SHA-256 hash of DER-encoded end-entity QSealC.
      // 32 bytes represented as 64 hex characters.
      "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // empty in this example

  // ES256 COSE signature: 64 bytes = 128 hex characters.
  "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

9. Use of cryptographic mechanisms

The use of cryptographic mechanisms in the context of this Annex shall be in compliance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by the European Union Agency for Cybersecurity (ENISA).

ANNEX III

NOTIFICATION OF INFORMATION REFERRED TO IN ARTICLE 6(2)

1. Member States shall provide the following information to the Commission on each competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities:

   (a) the name of the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities;

   (b) a registration number of the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities;

   (c) the contact email and contact phone number of the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities;

   (d) one or more certificates that can be used to verify the electronic seal created by the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities it issues, and for which the certified identity data include the name, and the registration number of the issuer, as specified in points (a) and (b), respectively;

   (e) the URL of the location where the issuer publishes the validity status of the physical versions of the European Disability Card or the European Parking Card for persons with disabilities.

2. Member States may provide the following information to the Commission on each competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities:

   (a) the URL of the webpage that contains the policies, terms and conditions of the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities that apply to the provision and use of the physical versions of the European Disability Card and the European Parking Card for persons with disabilities it provides;

   (b) where applicable, the URL of the webpage that contains additional information about the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities.

ANNEX IV

TECHNICAL SPECIFICATIONS FOR A REVOCATION LIST FOR THE PHYSICAL VERSIONS OF THE EUROPEAN DISABILITY CARD OR THE EUROPEAN PARKING CARD FOR PERSONS WITH DISABILITIES

1. For the purposes of this Annex, the identifier shall correspond to the revocation identifier (RID) defined in point 6 of Annex I and point 6 of Annex II.

2. A revocation list shall be implemented as an identifier list token in CWT (RFC 8392, section 7) format in accordance with Clause 5.2 of the token status list specification (draft-ietf-oauth-status-list-14) with the following amendments:

   (a) the value of the type claim shall be “application/identifierlist+cwt”;

   (b) the expiration time claim shall be present;

   (c) The StatusList claim shall not be present in the CWT claims set;

   (d) the IdentifierList structure defined in point 3 shall be present as a claim in the CWT claims set using the key 65530;

   (e) the CWT shall be a COSE_Sign1 object using, for calculating the signature, a signature algorithm in compliance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by the European Union Agency for Cybersecurity (ENISA);

   (f) the CWT shall contain the x5chain parameter as defined in RFC 9360 (section 2) in the protected header that contains the certificate or chain of certificates to verify the signature of the revocation list;

   (g) the extended key usage OID specified in the token status list specification (draft-ietf-oauth-status-list-14) may be used for the identifier list signing certificate and it is recommended that verifiers support the extended key usage OID specified in the token status list specification and that issuer authority infrastructures do not make the extended key usage field critical when using the extended key usage OID specified in the token status list specification.

3. The IdentifierList structure shall be a CBOR structure with the following Concise Data Definition Language (CDDL):

```
IdentifierList = {
   "identifiers" : { * Identifier => IdentifierInfo },
   ? "aggregation_uri" : Aggregation_uri,
   * tstr => RFU
}

IdentifierInfo = {
    (tstr / int) => RFU
}

Identifier = bstr
```

Aggregation_uri = tstr